* We propose a novel hybrid lightweight Attribute-Based Encryption (ABE) mechanism specifically designed for computationally constrained IoMT devices.
* We introduce an on-the-fly encryption scheme with embedded fine-grained access policies, eliminating the need for repeated re-encryption.
* We design a secure outsourced decryption approach that offloads decryption tasks to fog nodes without compromising data privacy.
* We implement the Advanced Message Queuing Protocol (AMQP) for the first time in this context to ensure secure, reliable, and low-latency data routing in IoMT networks.
* We propose an Intelligent Behavior-based Intrusion Detection System (IBIDS) that dynamically profiles node behavior for real-time anomaly detection.
* We develop a novel Pine Cone Optimization-based LightGBM model to effectively detect known threats with improved precision.
* We integrate a Self-Distilled Masked Autoencoder to enhance the detection of unknown and zero-day attacks through unsupervised behavior learning.
* We utilize a blockchain-based logging system to record access requests and policy enforcement actions, ensuring tamper-proof and decentralized auditability.